

# A Finite Presentation of CNOT-dihedral Operators

Matthew Amy, Jianxin Chen, Neil J. Ross

# Outline

Quantum circuits

Clifford+T and universal gate sets

CNOT-dihedral gates

Rules for CNOT-dihedral gates

Normal forms

Phase polynomials and uniqueness

Open questions

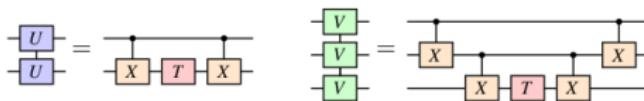
# CNOT-dihedral gates

In the paper, the CNOT-dihedral operators are defined as follows.

**Definition 3.1.** The *generators* are the scalar  $\omega = e^{i\pi/4}$  and the gates  $X$ ,  $T$ , and CNOT defined below.

$$\begin{array}{c} \text{---} \\ \boxed{X} \\ \text{---} \end{array} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{array}{c} \text{---} \\ \boxed{T} \\ \text{---} \end{array} = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix} \quad \begin{array}{c} \text{---} \\ \boxed{X} \\ \text{---} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

**Definition 3.2.** The *derived generators* are the gates  $U$  and  $V$  defined below.

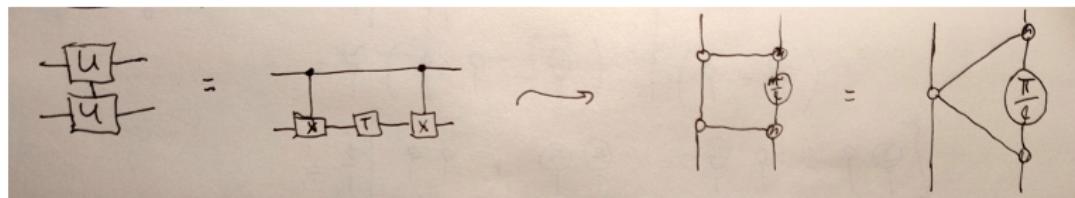
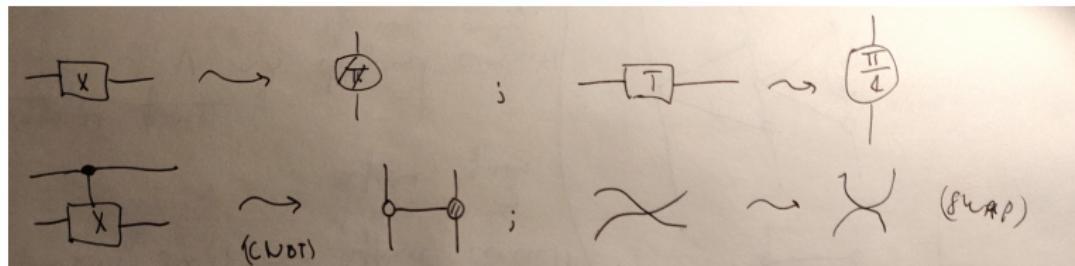
$$\begin{array}{c} \boxed{U} \\ \boxed{U} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \boxed{V} \\ \boxed{V} \\ \boxed{V} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array}$$


**Figure:** Amy, Chen and Ross, p. 86.

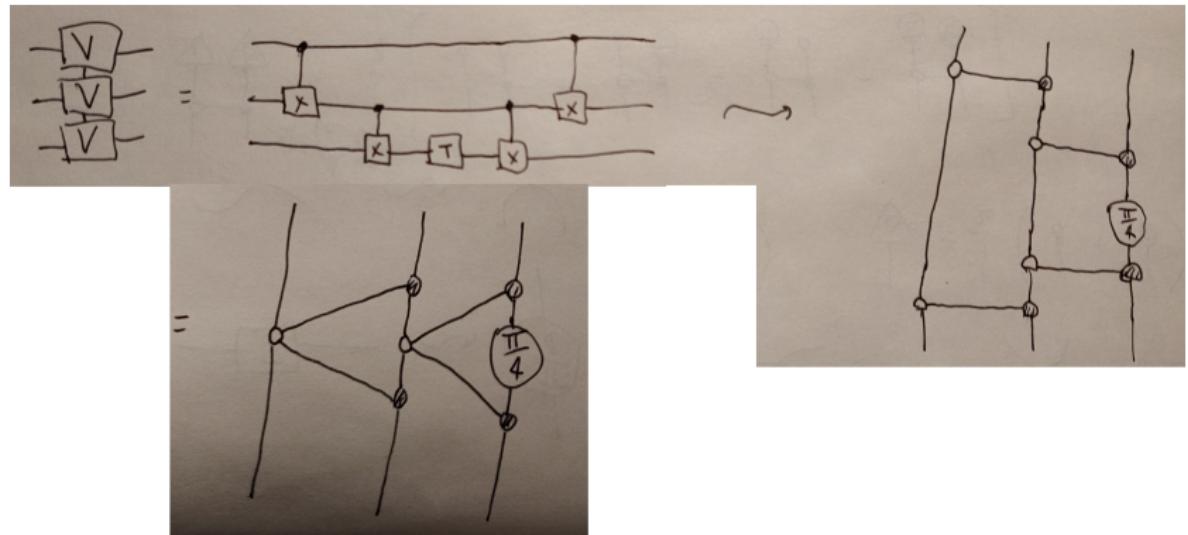
- ▶ The gates  $X$ ,  $CNOT$  and  $SWAP$  are called *affine*.
- ▶ The gates  $\omega$ ,  $T$ ,  $U$  and  $V$  are called *diagonal*.

# CNOT-dihedral gates in ZX

The gates can be expressed in the ZX-calculus.



# CNOT-dihedral gates in ZX



# Rules for CNOT-dihedral gates

$$R_1 : \boxed{X^2} = \underline{\hspace{1cm}}$$

$$R_2 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{X} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_3 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_4 : \begin{array}{c} \text{---} \\ | \\ \boxed{X^2} \\ | \\ \text{---} \end{array} = \underline{\hspace{1cm}}$$

$$R_5 : \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_6 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$R_7 : \boxed{T^8} = \underline{\hspace{1cm}}$$

$$R_8 : \begin{array}{c} \boxed{U^4} \\ | \\ \boxed{U^4} \end{array} = \begin{array}{c} \boxed{T^4} \\ | \\ \boxed{T^4} \end{array}$$

$$R_9 : \begin{array}{c} \boxed{V^2} \\ | \\ \boxed{V^2} \\ | \\ \boxed{V^2} \end{array} = \begin{array}{c} \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \\ | \\ \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \\ | \\ \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \end{array}$$

$$R_{10} : \omega^8 =$$

$$R_{11} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{T} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \omega \begin{array}{c} \text{---} \\ | \\ \boxed{T^7} \\ | \\ \text{---} \end{array}$$

$$R_{12} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{T} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{T} \\ | \\ \text{---} \end{array}$$

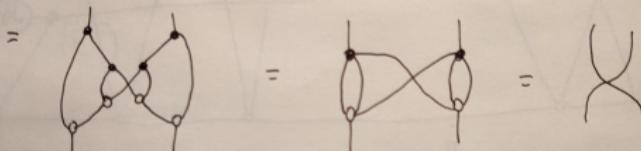
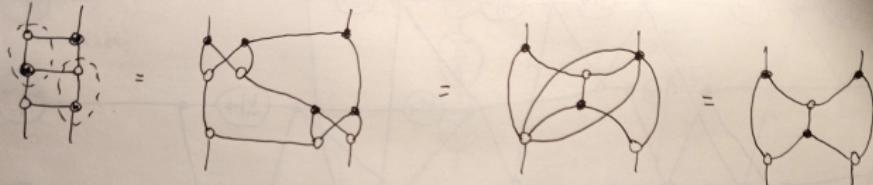
$$R_{13} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{V} \quad \boxed{X} \\ | \\ \boxed{V} \\ | \\ \boxed{V} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \end{array}$$

Figure 1: The relations.  $R_1$  through  $R_6$  are affine relations.  $R_7$  through  $R_{10}$  are diagonal relations.  $R_{11}$  through  $R_{12}$  are commutation relations.

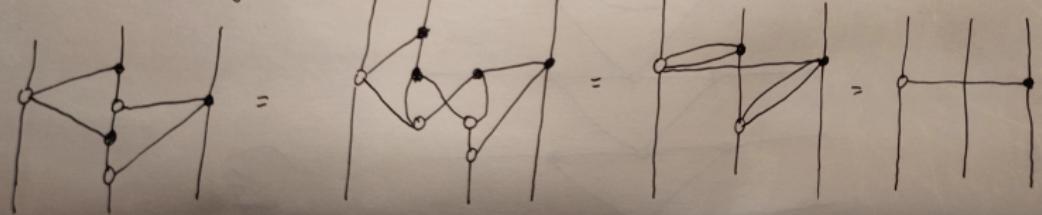
**Figure:** Amy, Chen and Ross, p. 87.

# Derivation of R5 and R6 in ZX

derivation of R<sub>5</sub> (in ZX)



derivation of R<sub>6</sub>



## Commutation rules

$$-\boxed{X} \boxed{T} - = \omega \cdot -\boxed{T^\top} \boxed{X} -$$

$$\begin{array}{c} \text{---} \\ | \quad | \\ \boxed{X} \quad \boxed{V} \\ | \quad | \\ \text{---} \end{array} = \omega \cdot \begin{array}{c} \text{---} \\ | \quad | \\ \boxed{V^\top} \quad \boxed{X} \\ | \quad | \\ \text{---} \end{array}$$

$$\begin{array}{c} X \\ \text{---} \\ U \\ \text{---} \\ U \end{array} = \omega \cdot \begin{array}{c} U^\top \\ \text{---} \\ U^\top \\ \text{---} \\ X \end{array}$$

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{X} \boxed{V} \boxed{V} = \omega \cdot \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{V^T} \boxed{V^T} \boxed{X} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{U} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \omega \cdot \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{U^\dagger} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \boxed{V} \\ \text{---} \\ \text{---} \\ \boxed{V} \\ \text{---} \\ \text{---} \\ \boxed{X} \\ \text{---} \\ \boxed{V} \\ \text{---} \end{array} = \omega \cdot \begin{array}{c} \text{---} \\ \text{---} \\ \boxed{V^\top} \\ \text{---} \\ \text{---} \\ \boxed{V^\top} \\ \text{---} \\ \text{---} \\ \boxed{V^\top} \\ \text{---} \\ \boxed{X} \\ \text{---} \end{array}$$

$$\begin{array}{c} \text{---} \\ | \\ \boxed{X} \end{array} \quad \boxed{T} \quad = \quad \boxed{T} \quad \begin{array}{c} \text{---} \\ | \\ \boxed{X} \end{array}$$

A quantum circuit diagram showing three horizontal lines. The top line has a small square box containing the letter  $X$ . To its right are two blue rectangular boxes, each containing the letter  $U$ , stacked vertically.

$$\begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{T} \end{array} = \begin{array}{c} \boxed{U} \\ \boxed{U} \\ \text{---} \\ | \\ \boxed{X} \end{array}$$

$$\begin{array}{c} X \\ \square \\ U \end{array} = \begin{array}{c} T \\ \square \\ X \end{array}$$

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{X} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{V} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{U} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{X} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

**T**

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{V} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \boxed{U} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$\begin{array}{c} V \\ \hline V \\ \hline V \\ \hline X \end{array} = \begin{array}{c} V \\ \hline V \\ \hline V \\ \hline X \end{array}$$

$$\text{---} \times \text{---} = \text{---} \times \text{---}$$

$$\text{---} = \boxed{U}$$

$$\text{---} \times \text{---} = \text{---} \times \text{---}$$

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \text{---} \end{array}$$

$$\text{---} \otimes \begin{array}{|c|} \hline U \\ \hline U \\ \hline \end{array} = \begin{array}{|c|} \hline U \\ \hline U \\ \hline \end{array} \otimes \text{---}$$

$$\begin{array}{c} \text{---} \\ | \\ \square V \\ | \\ \square V \end{array} = \begin{array}{c} \text{---} \\ | \\ \square V \\ | \\ \square V \end{array}$$

$$\begin{array}{c} V \\ \square \\ V \end{array} = \begin{array}{c} V \\ \square \\ V \end{array}$$

$$\begin{array}{c} \text{X} \\ \diagdown \\ \text{V} \\ \diagup \\ \text{V} \end{array} = \begin{array}{c} \text{V} \\ \diagup \\ \text{X} \\ \diagdown \end{array}$$

$$\begin{array}{c} \text{---} \\ | \\ \boxed{V} \\ | \\ \boxed{V} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{V} \\ | \\ \text{---} \end{array}$$

## Phase polynomials

Action of a diagonal gate:

$$D |x\rangle = \omega^{p_D(x)} |x\rangle, \quad p_D : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_8,$$

$$p_D(x) = \sum_{i=1}^k a_i g_i(x).$$

where  $a_i \in \mathbb{Z}_8$  and  $g_i : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  are terms on at most  $n$  variables.

$$\omega^k |x\rangle = \omega^k |x\rangle$$

$$T^k |x_1\rangle = \omega^{kx_1} |x_1\rangle$$

$$U^k |x_1 x_2\rangle = \omega^{k(x_1 \oplus x_2)} |x_1 x_2\rangle$$

$$V^k |x_1 x_2 x_3\rangle = \omega^{k(x_1 \oplus x_2 \oplus x_3)} |x_1 x_2 x_3\rangle$$

Therefore for  $D$  in normal form we have

$$p_D(x) = a_0 + \sum_i a_i x_i + \sum_{i < j} b_{ij}(x_i \oplus x_j) + \sum_{i < j < k} c_{ijk}(x_i \oplus x_j \oplus x_k)$$

Where  $a_i \in \mathbb{Z}_8$ ,  $b_{ij} \in \mathbb{Z}_4$ ,  $c_{ijk} \in \mathbb{Z}_2$  (from the bounds on  $\deg_x(D)$  for  $X = T, U, V$  obtained in normal form).

## Uniqueness

Suppose  $D$  and  $D'$  are distinct diagonal normal forms, then by construction  $p_D(x) \neq p_{D'}(x)$  as polynomials. However this does not mean that  $\exists y \in \mathbb{Z}_2^n$  s.t.  $p_D(y) \neq p_{D'}(y)$ .

Counterexample:  $4x_1 + 4x_2 + 4(x_1 \oplus x_2) = 0 \bmod 8$  for any  $x_1, x_2 \in \mathbb{Z}_2$

To show there exists such a  $y$  need a technical lemma: construct a multilinear polynomial  $q : \mathbb{Z}_8^n \rightarrow \mathbb{Z}_8$  such that  $p_D(y) - p_{D'}(y) = q(y) \forall y \in \mathbb{Z}_2^n$ .

Do this by translating from mod 2 to mod 8:

$$x_i \oplus x_j = x_i + x_j - 2x_i x_j$$

$$x_i \oplus x_j \oplus x_k = x_i + x_j + x_k - 2x_i x_j - 2x_i x_k - 2x_j x_k + 4x_i x_j x_k$$

Then  $p_D(x) - p_{D'}(x) \neq 0 \implies q(x) \neq 0$ , because of the bounds on  $a_i$ ,  $b_{ij}$  and  $c_{ijk}$ . Pick a non-zero term  $d x_{i_1} \dots x_{i_k}$  in  $q(x)$  then letting  $y$  be the vector with 1's in  $i_j$ th positions and zero everywhere else we obtain  $q(y) = d \neq 0$  and so  $D|y\rangle \neq D'|y\rangle$ .

## Open questions

- ▶ Interaction between ZX and CNOT-dihedral rules (rule 13?)
- ▶ The paper doesn't contain an algorithm for normalizing CNOT-dihedral circuits, it uses the properties of the ambient symmetric monoidal structure non-constructively. What could be a rewrite system? Algebraic vs combinatorial description.
- ▶ Complexity of CNOT-dihedral circuits.